LES GUIDES DE LA CNIL



GUIDE

POUR LES EMPLOYEURS ET LES SALARIÉS

Édition 2008



Sommaire

Ce guide est téléchargeable sur le site Internet de la CNIL : www.cnil.fr

Avant-propos

Les entreprises et les administrations recourent de façon croissante aux moyens informatiques pour gérer leurs ressources humaines. L'ensemble du secteur des RH est concerné : recrutement, gestion des carrières et des compétences, le suivi du temps de travail, etc..

Simultanément, les dispositifs de contrôle des salariés liés aux nouvelles technologies se multiplient : vidéosurveillance, cybersurveillance, applications biométriques, géolocalisation, etc..

Ces applications enregistrent de nombreuses informations à caractère personnel sur les salariés. La loi Informatique et Libertés fixe un cadre à la collecte et au traitement de ces données afin de les protéger, dans la mesure où leur divulgation ou leur mauvaise utilisation est susceptible de porter atteinte aux droits et libertés des personnes, ou à leur vie privée.

Le respect, par les entreprises et administrations des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard des salariés. C'est aussi un gage de sécurité juridique pour les employeurs qui sont responsables de ces traitements informatiques et de la sécurité des données personnelles qu'ils contiennent. Ils peuvent ainsi voir leur responsabilité, notamment pénale, engagée en cas de non-respect des dispositions de la loi.

C'est pourquoi notre commission, chargée de veiller au respect de ces principes, souhaite informer les salariés des droits dont ils disposent, ainsi que les employeurs, en les conseillant sur les mesures à adopter pour se conformer à la loi.

Ce guide a pour vocation de leur donner les clés pour bien utiliser ces outils et les fichiers mis en œuvre en matière de gestion des ressources humaines.

C'est aussi le but du « correspondant informatique et libertés », interlocuteur privilégié de la CNIL dont la désignation permet, au-delà de l'exonération de déclaration, d'intégrer pleinement la problématique de la protection des données personnelles.

Alex TÜRK
Président de la CNIL

I – Les 5 principes clés à respecter

La loi « Informatique et Libertés » du 6 janvier 1978 modifiée par la loi du 6 août 2004 est applicable dès lors qu'il existe un traitement automatisé ou un fichier manuel (c'est-à-dire un fichier informatique ou un fichier « papier ») contenant des informations relatives à des personnes physiques.

Elle définit les principes à respecter lors de la collecte, du traitement et de la conservation de ces données et garantit un certain nombre de droits pour les personnes.

1. Le principe de finalité

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage **déterminé et légitime**.

- *la mise en place d'un autocommutateur téléphonique ou d'un dispositif de localisation par GPS (géolocalisation) ne peut avoir pour objectif le contrôle des conversations téléphoniques ou des déplacements de salariés protégés.*
- *Le fichier du personnel et l'adresse électronique des employés ne peut être utilisé à des fins de propagande politique. Les informations enregistrées par un logiciel conçu pour la réservation de billets de transports et déclaré comme tel ne peuvent être utilisées par un employeur pour contrôler l'activité de ses salariés (Cour d'appel de Paris, ch. Soc., 31 mai 1995).*

Tout détournement de finalité est passible de sanctions pénales.

Les objectifs poursuivis par la mise en place d'une application informatique doivent donc être au préalable clairement définis (gestion des recrutements, sécurité du réseau informatique, contrôle du temps de travail, etc.).

2. Le principe de proportionnalité et de pertinence des données

Seules doivent être traitées les informations **pertinentes et nécessaires** au regard des objectifs poursuivis.

Par exemple : le recueil d'informations sur l'entourage familial, l'état de santé ou encore le numéro de sécurité sociale d'un candidat à un recrutement n'est pas pertinent. L'enregistrement de la situation familiale précise d'un salarié ne peut se justifier que pour l'attribution d'avantages sociaux particuliers au salarié ou à sa famille.

En outre, comme le rappelle le code du travail, la mise en place d'un dispositif de contrôle des salariés ne doit pas conduire à apporter aux droits et libertés des personnes de restrictions qui ne seraient pas **proportionnées** au but recherché et justifiées par l'intérêt légitime de l'entreprise (article L1121-1 du code du travail).

Par exemple : la mise sous vidéosurveillance permanente d'un poste de travail ne pourrait intervenir qu'en cas de risque particulier et dûment avéré pour la sécurité du salarié concerné (voir fiche n° 8). De même, la mise en place, pour contrôler l'accès à des locaux d'une base d'empreintes digitales ne peut se justifier que face à un fort impératif de sécurité et en l'absence de solutions alternatives moins intrusives (voir fiche n° 12).

3. Le principe d'une durée limitée de conservation des données

Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation précise doit être déterminée en fonction de la finalité de chaque fichier.

Par exemple : le temps de la présence du salarié s'agissant d'une application de gestion des carrières, cinq ans pour un fichier de paie, deux ans après le dernier contact avec le candidat à un emploi pour un fichier de recrutement, un mois pour les enregistrements de vidéosurveillance…

4. Le principe de sécurité et de confidentialité des données

L'employeur, en tant que responsable du traitement, est astreint à une **obligation de sécurité** : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non autorisés.

Par exemple : chaque salarié doit disposer d'un mot de passe individuel régulièrement changé. Les droits d'accès aux données doivent être précisément définis en fonction des besoins réels de chaque personne (lecture, écriture, suppression). Il peut également être utile de prévoir un mécanisme de verrouillage systématique des postes informatiques au-delà d'une courte période de veille.

Ainsi, les données à caractère personnel ne doivent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions.

Par exemple : les personnes habilitées du service des ressources humaines s'agissant de la gestion de la paie, les administrateurs réseaux s'agissant des données de connexion à internet.

Les données peuvent néanmoins être communiquées à des tiers autorisés à en connaître en application de dispositions législatives particulières (Inspections du travail, services fiscaux, services de police…).

5. Le principe du respect des droits des personnes

> Information des personnes

Lors de l'informatisation de leurs données, les salariés concernés ou les candidats à un emploi doivent être **clairement informés** des objectifs poursuivis, du caractère obligatoire ou facultatif de leurs réponses, des destinataires des données et des modalités d'exercice de leurs droits au titre de la loi « Informatique et Libertés » (droit d'accès, de rectification et d'opposition).

Cette information peut être diffusée par tout moyen approprié : panneaux d'affichage ; page « protection des données » ou « informatique et libertés » sur l'intranet de l'entreprise.

En outre, lorsque les données sont recueillies par voie de questionnaires, papier ou informatisé, ceux-ci doivent comporter cette information.

Au-delà, l'employeur doit s'assurer du respect des procédures de consultation et d'information obligatoires des instances représentatives du personnel.

Enfin, l'employeur doit adresser une déclaration préalable à la CNIL sauf, pour les traitements les plus courants, en cas de désignation d'un « correspondant informatique et libertés ».

> Droits d'accès et de rectification

Toute personne peut demander au détenteur d'un fichier de lui **communiquer** toutes les informations la concernant contenues dans ce fichier. Elle a également le droit de faire **rectifier ou supprimer** les informations erronées.

Par exemple : un salarié peut accéder à son dossier professionnel (voir fiche n° 3).

> Droit d'opposition

Toute personne a le droit de **s'opposer, pour des motifs légitimes** à ce que des données à caractère personnel la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci résulte d'une obligation légale ou réglementaire (ex. : déclarations sociales obligatoires, tenue du registre du personnel).

Par exemple : une personne peut dans certaines conditions s'opposer à la mise en ligne de ses coordonnées professionnelles ou de sa photographie (voir fiche n° 2).

II – Les missions de la CNIL

La Commission nationale de l'informatique et des libertés, autorité administrative indépendante est chargée d'assurer le respect des dispositions de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004.

1. Le rôle de conseil et d'information

La CNIL conseille et renseigne les personnes et les organismes qui envisagent de mettre en œuvre des fichiers informatiques, que ce soit par téléphone, par courrier ou par ses publications. Elle s'est dotée d'un service d'orientation et de renseignement afin d'apporter une réponse rapide aux requêtes des particuliers comme des professionnels sur l'application de la loi.

2. Le contrôle de la conformité des fichiers à la loi

La CNIL vérifie, lors de l'instruction des déclarations de fichiers qui lui sont adressées, que les caractéristiques des traitements concernés sont bien conformes à la loi et autorise la mise en œuvre des traitements qui, aux termes de la loi, nécessitent une attention particulière du fait de leur contenu ou de leur finalité. Elle peut simplifier les formalités déclaratives, voire exonérer de déclaration certains fichiers.

La CNIL reçoit les plaintes concernant le non-respect de la loi.

La CNIL dispose d'un pouvoir de contrôle qui permet à ses membres et ses agents d'accéder à tous les locaux professionnels. Sur place, ses membres et agents peuvent demander communication de tout document nécessaire et en prendre copie, recueillir tout renseignement utile et accéder aux programmes informatiques et aux données.

3. Le pouvoir de sanction

Au titre de son pouvoir de sanction, la CNIL peut notamment :

- adresser des avertissements et des mises en demeure de faire cesser un manquement à la loi ;
- prononcer une injonction de cesser le traitement ou un retrait de l'autorisation et, en cas d'urgence, décider l'interruption du traitement ou le verrouillage des données ;
- prononcer des sanctions pécuniaires pouvant aller jusqu'à 300 000 € en cas de réitération ;
- dénoncer au parquet les infractions à la loi dont elle a connaissance.

III – Le correspondant (CIL) : un vecteur de diffusion de la culture informatique et libertés

Institué en 2004 à l'occasion de la refonte de la loi du 6 janvier 1978, le correspondant à la protection des données ou correspondant informatique et libertés (CIL) est un acteur et un relais incontournable de la culture « informatique et libertés ».

Le correspondant doit, si possible, être un employé du responsable de traitement (correspondant interne), car connaissant mieux, a priori, l'activité et le fonctionnement interne de son entreprise ou de son administration, il est à même de veiller en temps réel à la bonne application des règles et des conditions de mise en œuvre des traitements. Mais il est aussi possible de désigner un correspondant n'appartenant pas à l'organisme (correspondant externe).

Pour s'acquitter de sa tâche, quel que soit son statut, le correspondant « informatique et libertés » doit disposer de la liberté d'action et des moyens qui lui permettront de recommander des solutions organisationnelles ou techniques adaptées. Il doit pouvoir exercer pleinement ses missions, en dehors de toute pression, et jouer son rôle auprès du responsable de traitement.

Le CIL – Quelques informations pratiques

Pourquoi désigner un CIL ? : Sa désignation, qui est facultative, exonère de déclaration la plupart des fichiers. Il contribue à une meilleure application de la loi.

Quels avantages pour l'organisme ? : Le CIL est un acteur de la sécurité juridique au sein de l'organisme. Son action peut prendre plusieurs formes : le conseil, la recommandation, la sensibilisation, la médiation et l'alerte en cas de disfonctionnement.

Comment désigner un CIL ? : C'est simple, il suffit de remplir le formulaire téléchargeable sur le site internet de la CNIL.

Comment le CIL pourrait-il/elle être formé(e) ? : La CNIL propose des ateliers d'information gratuits, généralistes et thématiques, animés par ses propres experts.

Quelle relation avec la CNIL ? : La CNIL a mis en place un service spécifique pour garantir au CIL une réponse rapide et de qualité. Il s'agit d'un guichet unique pour toutes les questions juridiques ou les éclairages liés à l'exercice de la fonction.

D'autres avantages ? : Le CIL est un interlocuteur privilégié de la CNIL. Ses demandes sont donc traitées en priorité. Il fait partie du réseau des CIL animés par la CNIL. Il participe à la réflexion liée à l'évolution de la fonction, à la création d'outils de travail, des textes juridiques…

Fiche n° 1 – les opérations de recrutement

1. Quelles sont les données qui peuvent être collectées ?

Les informations demandées sous quelque forme que ce soit, au candidat à un emploi ont pour finalité d'apprécier sa capacité à occuper l'emploi proposé. Elles doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles du candidat.

La collecte des informations suivantes n'est pas pertinente, sauf cas particuliers justifiés par la nature très spécifique du poste à pourvoir ou par une obligation légale :

- date d'entrée en France ;
- date de naturalisation ;
- modalités d'acquisition de la nationalité française ;
- nationalité d'origine ;
- numéros d'immatriculation ou d'affiliation aux régimes de sécurité sociale ;
- détail de la situation militaire : sous la forme « objecteur de conscience, ajourné, réformé, motifs d'exemption ou de réformation, arme, grade » ;
- adresse précédente ;
- entourage familial du candidat (nom, prénom, nationalité, profession et employeur du conjoint ainsi que nom, prénom, nationalité, profession, employeur, des parents, des beaux-parents, des frères et sœurs et des enfants) ;
- état de santé, taille, poids, vue ;
- conditions de logement (propriétaire ou locataire) ;
- vie associative ;
- domiciliation bancaire, emprunts souscrits.

Enfin, il est interdit de collecter et de conserver des données personnelles qui, directement ou indirectement, font apparaître les **origines raciales** ou **ethniques**, les **opinions politiques**, **philosophiques** ou **religieuses** ou les **appartenances syndicales**, les informations relatives à la santé ou à la vie sexuelle des personnes. L'accord exprès exigé par la loi qui doit être recueilli par écrit ne saurait, à lui seul, justifier la collecte de telles données si ces dernières sont dépourvues de lien direct et nécessaire avec l'emploi proposé. Aussi de telles informations ne peuvent-elles être collectées que, dans certains cas, lorsqu'elles sont dûment justifiées par la spécificité du poste à pourvoir.

Le recueil de références auprès de l'environnement professionnel du candidat (supérieurs hiérarchiques, collègues, maîtres de stages, clients, fournisseurs…) est permis dès lors que le candidat en a été préalablement informé.



Attention

Les « zones commentaires » destinées à enregistrer des informations de gestion, telles des résumés d'entretien, doivent, comme toute donnée à caractère personnel enregistrée dans un traitement être pertinentes, adéquates et non excessives au regard de la finalité du traitement. La CNIL veille au respect de ces principes. Il faut avoir à l'esprit en rédigeant ces zones commentaires que la personne concernée peut y avoir accès à tout moment. Ainsi, à la suite d'un contrôle sur place effectué par une délégation de la CNIL en décembre 2006, il a été constaté que des commentaires particulièrement subjectifs, relatifs aux personnes ayant déjà été employées par une société mais qui n'ont pas donné satisfaction, figuraient dans le traitement de gestion des salariés qu'elle avait mis en œuvre. Ainsi, ont pu être relevés des commentaires tels que *« trop chiante », « problèmes d'hygiène (odeurs) », « personne sans dents et qui boit »*. Conformément aux articles 45 et suivants de la loi du 6 janvier 1978 modifiée, la formation contentieuse de la CNIL a prononcé, le 11 décembre 2007, une sanction pécuniaire d'un montant de 40 000 euros à l'encontre de cette société, compte tenu de la gravité des manquements constatés *(Délibération n° 2007-374 du 11 décembre 2007).*

2. L'information des candidats

Lors de la collecte des données, les candidats doivent être informés :

- de l'identité du responsable du traitement (ex : cabinet de recrutement X ; service des ressources humaines de la société Y) ;
- des finalités du traitement (ex : gestion des candidatures) ;
- du caractère obligatoire ou facultatif des réponses, (ex : le recueil d'informations sur les loisirs est facultatif) ;
- des conséquences à leur égard d'un défaut de réponse ;
- des personnes physiques ou morales destinataires des informations (ex : autres cabinets de recrutements) ;
- des conditions d'exercice de leur droit d'accès et de rectification ainsi que de leur droit d'opposition (ex : indication du service auprès duquel ces droits peuvent être exercés).

Attention

Lorsque des informations sur un candidat sont recueillies par voie de questionnaires papier ou de formulaires en ligne, ceux-ci doivent porter mention de ces prescriptions de façon claire et lisible (voir modèle proposé en annexe).



La CNIL recommande que les personnes chargées du recrutement prennent toutes les dispositions nécessaires pour informer le candidat, dans un délai raisonnable :

- des suites données à sa candidature;
- de la durée de conservation des informations le concernant ainsi que de la possibilité d'en demander la restitution ou la destruction;
- de toute éventuelle cession d'informations avec d'autres organismes de recrutement et de la possibilité de s'y opposer;
- des méthodes et techniques d'aide au recrutement utilisées à son égard. Les résultats obtenus doivent rester confidentiels. Les méthodes et techniques d'aide au recrutement ou d'évaluation des candidats à un emploi doivent être pertinentes au regard de la finalité poursuivie. La Commission recommande que l'information concernant les méthodes d'aide au recrutement employées soit dispensée préalablement par écrit sous une forme individuelle ou collective.

Lorsque l'identité de l'employeur n'a pas été précisée lors de l'offre de poste, il est recommandé que l'accord du candidat soit recueilli préalablement à la transmission de son CV à cet employeur.

Dans le cas de sites de recrutements en ligne, la CNIL recommande que le candidat à l'emploi soit informé de la forme, nominative ou non, sous laquelle les informations le concernant seront éventuellement diffusées en ligne ou transmises aux employeurs.

3. Comment exercer ses droits ?

Tout candidat ou employé doit pouvoir obtenir sur demande et dans un délai raisonnable toutes les informations le concernant y compris les résultats des analyses et des tests (psychologiques, graphologiques...) ou évaluations professionnelles éventuellement pratiqués.

Le droit d'accès s'applique aux informations collectées directement auprès du candidat, aux informations éventuellement collectées auprès de tiers ainsi qu'aux informations issues des méthodes et techniques d'aide au recrutement.

La Commission recommande que la communication des informations contenues dans la fiche du candidat soit effectuée par écrit. La communication des résultats des tests ou évaluations peut être faite par tout moyen approprié au regard de la nature de l'outil utilisé.

En cas de contestation portant sur l'exactitude des informations, la charge de la preuve incombe au service auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les informations contestées ont été communiquées par la personne concernée ou avec son accord.

4. Combien de temps peut-on conserver les données relatives à un candidat ?

La CNIL recommande que la durée de conservation des informations (sur support informatique et papier) n'excède pas **deux ans** après le dernier contact avec la personne concernée.

5. Comment déclarer ?

Les applications de gestion du recrutement doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration normale, sauf désignation d'un correspondant informatique et libertés (dispense de déclaration).

Fiche n° 2 – les annuaires du personnel

La constitution d'un annuaire du personnel sur support informatisé comportant l'identité des salariés, leur fonction, leurs coordonnées professionnelles et le cas échéant leur photographie, constitue un traitement de données personnelles soumis aux dispositions de la loi du 6 janvier 1978 modifiée en 2004.

Les annuaires du personnel ne doivent pas être utilisés à des fins commerciales ou politiques.

Distinction annuaire interne/annuaire « externe »

Annuaire interne : annuaire accessible aux seuls membres du personnel, diffusé sur intranet ou sur format papier.

Annuaire « externe » : annuaires accessibles à d'autres personnes que le personnel de l'organisme (ex : annuaire publié sur internet).

1. La nécessité d'informer les intéressés

L'employeur doit informer ses salariés, préalablement à la mise en place d'un annuaire, de leurs droits d'accès, de rectification et d'opposition. Cette information s'effectue par la remise d'un document écrit ou par voie électronique (voir modèle proposé en annexe).

La diffusion sur internet de données à caractère personnel (ex : nom, prénom, coordonnées professionnelles, etc.) rend ces informations accessibles à quiconque, sans que l'intéressé puisse réellement maîtriser leur utilisation. Par conséquent, le salarié doit pouvoir s'opposer simplement et à tout moment à une telle diffusion.

La CNIL recommande que la diffusion de la photographie soit subordonnée à l'accord préalable de l'employé en particulier lorsque cette photographie est destinée à être publiée ou mise en ligne sur internet.

2. Comment déclarer ?

Les annuaires professionnels internes doivent faire l'objet d'une déclaration de conformité en référence à la norme n° 46 relative à la gestion des personnels des organismes publics et privés, sauf si un Correspondant informatique et libertés a été désigné au sein de l'organisme (dispense de déclaration).

Les annuaires autres que les annuaires internes doivent faire l'objet d'une déclaration normale préalablement à leur mise en œuvre, sauf si un Correspondant informatique et libertés a été désigné au sein de l'organisme (dispense de déclaration).

Fiche n° 3 – l'accès au dossier professionnel

Tout salarié ou ancien salarié justifiant de son identité a le droit d'accéder à son dossier professionnel auprès du service du personnel.

1. Un droit d'accès à quelles données ?

L'intéressé peut obtenir communication de l'ensemble des données le concernant, qu'elles soient conservées sur support informatique ou dans un dossier papier.

Par exemple, il a le droit d'accéder aux données relatives :

- à son recrutement;
- à son historique de carrière;
- à sa rémunération;
- à l'évaluation de ses compétences professionnelles (entretiens annuels d'évaluation, notation);
- à son dossier disciplinaire, etc.

2. Limites au droit d'accès

Le salarié ou ancien salarié n'a pas le droit d'accéder :

- aux données concernant la situation personnelle d'un tiers, notamment d'un autre salarié;
- aux données prévisionnelles de carrière (potentiel de carrière, classement), sauf si ces données ont été prises en compte pour décider de son augmentation de salaire, de sa promotion, de son affectation, etc. Un salarié doit ainsi pouvoir accéder à l'ensemble des données de gestion des ressources humaines qui ont servi à prendre une décision à son égard.

L'employeur a le droit de s'opposer aux demandes manifestement abusives. En cas de contestation, il doit démontrer que la demande du salarié est abusive.

3. Comment s'exerce le droit d'accès ?

Le droit d'accès peut s'exercer soit sur place, soit par écrit, avec un justificatif d'identité.

L'employeur doit répondre immédiatement si la demande est effectuée sur place, ou dans un délai maximal de 2 mois si la demande est écrite (ou s'il est impossible de répondre immédiatement à la demande sur place). Son éventuel refus doit être écrit, motivé et doit mentionner les voies et délais de recours.

Une copie des données est délivrée à l'intéressé à sa demande. Le simple coût de la copie peut éventuellement lui être réclamé.

Les codes, sigles et abréviations figurant dans les documents communiqués doivent être expliqués, si nécessaire à l'aide d'un lexique.

Fiche n° 4 – la gestion des œuvres sociales et culturelles

Qu'il s'agisse de la gestion des subventions, des bourses, des primes de crèches, des chèques cadeaux, des activités de voyages, sport ou loisirs, les traitements informatisés mis en œuvre par les comités d'entreprise (CE) ou d'établissement, ainsi que par les comités centraux d'entreprises, les comités de groupe, les comités interentreprises ou les délégués du personnel, enregistrent des données personnelles sur les salariés et doivent à ce titre se conformer à la loi informatique et libertés.
Ces informations doivent être limitées à celles qui sont strictement nécessaires au CE pour exercer ses fonctions légales.

Par exemple : Le CE peut être amené à demander la fourniture de la copie de l'avis d'imposition des ouvrants droit afin de procéder au calcul de la contribution de chacun en fonction de ses ressources. En revanche, le CE ne peut exiger la production de la déclaration de revenus, qui comporte des informations relevant de la vie privée des intéressés (Cour de Cassation, chambre civile, arrêt du 29 mai 1984, n° 82-12.232).

1. Information des salariés

Les salariés doivent être préalablement informés par le CE, et le cas échéant l'employeur, de l'objectif poursuivi, des destinataires des données, ainsi que de l'identité de la personne ou du service auquel ils peuvent s'adresser pour exercer leurs droits d'accès, de rectification et d'opposition (voir modèles proposés en annexe).

Par exemple : affichage d'une note d'information dans les locaux, remise d'un document à l'employé, mentions apparentes sur le questionnaire.

2. Droit d'opposition

- Tout salarié a le droit de s'opposer à ce que le CE soit rendu destinataire de données le concernant par l'employeur. La transmission de ces données au CE ne peut être que facultative, le salarié devant être clairement informé des conséquences d'un éventuel refus de sa part;

  Par exemple : application du tarif le plus élevé ou exclusion du bénéfice d'une prestation.

- Lorsque les données sont utilisées à des fins d'offres promotionnelles les personnes concernées sont informées qu'elles peuvent s'y opposer sans frais et sans justification. L'envoi d'offres promotionnelles par voie électronique est subordonné au recueil du consentement préalable des personnes concernées.

3. Comment déclarer ?

Les traitements de gestion sociale ou culturelle les plus courants sont dispensés de déclaration. Pour bénéficier de cette dispense, les traitements envisagés doivent être conformes à la dispense de déclaration n°10 en date du 17 octobre 2006 (disponible sur www.cnil.fr).

Dans tous les autres cas, le CE doit adresser à la CNIL une déclaration normale.

4. Droits de mise à jour ou de suppression des données

S'il constate la présence de données erronées ou interdites (ex. : appréciations subjectives, opinions politiques, sanctions amnistiées…), le salarié ou ancien salarié a le droit de demander la mise à jour ou la suppression de ces données.

Si ces données ont été transmises à des tiers (à d'autres entreprises du groupe par exemple), l'employeur doit demander à ces tiers leur mise à jour ou leur suppression.

L'intéressé peut demander à l'employeur de justifier, sans frais, qu'il a bien pris en compte ses demandes de rectification ou de suppression des données. Il peut également obtenir le remboursement des frais de copie que l'employeur lui a éventuellement réclamés.

5. Que faire en cas de difficulté ?

Il est possible d'alerter le correspondant informatique et libertés (CIL) qui a pu être désigné par l'employeur ou de saisir la CNIL d'une plainte. Une plainte pénale peut également être déposée auprès du Procureur de la République ou des services de police ou de gendarmerie.

Fiche n° 5 – les transferts internationaux de données

1. De quoi s'agit-il ?

Constitue un transfert de données vers un pays tiers toute communication ou copie de données par l'intermédiaire d'un réseau, ou d'un support à un autre, quel que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire.

Par exemple : sont considérés comme des transferts internationaux de données :

- *la centralisation dans un pays étranger de la base de données de gestion des ressources humaines ;*
- *le transfert vers un prestataire étranger aux fins de saisie informatique des dossiers du personnel ;*
- *l'hébergement de données à caractère personnel dans un pays étranger.*

2. Pourquoi encadrer les transferts de données à caractère personnel vers des pays n'appartenant pas à l'Union européenne ?

Les personnes bénéficiant d'une protection de leurs données en France par la loi « Informatique et Libertés » doivent continuer à en bénéficier lorsque leurs données quittent le territoire français pour faire l'objet d'un traitement en dehors de l'Union européenne.

3. Quelles sont les principales obligations à respecter ?

> Finalité

Tout transfert de données vers l'étranger doit avoir une finalité déterminée, explicite et légitime : le responsable de traitement établi en France doit pouvoir expliquer pourquoi le transfert a lieu (ex : transfert d'information à destination de la maison mère, hébergement des données à l'étranger, externalisation de certains services…) et s'être assuré que ces raisons sont compatibles avec les exigences de la loi française (ex : sécurité des données, durée de conservation limitée des données…).

Les données transférées ne doivent pas être traitées ultérieurement de manière incompatible avec cette finalité.

> Pertinence des données

Les données transférées doivent être adéquates, pertinentes et non excessives au regard de la ou des finalités pour lesquelles elles sont transférées.



Concernant cette dernière obligation, la CNIL constate fréquemment que des sociétés multinationales envisagent d'opérer des transferts concernant l'intégralité du personnel de sociétés françaises dans le cadre de la centralisation des bases de données « ressources humaines » de leur groupe.
Ces transferts ne devraient pas porter sur la totalité ou la quasi-totalité des informations nominatives relatives aux salariés. En particulier le numéro de sécurité sociale, ou les données touchant à des aspects de la vie privée des employés (ex : détails sur la situation familiale, coordonnées bancaires) paraissent a priori ne devoir relever que d'une gestion locale.

> Information des salariés
Outre les dispositions législatives concernant la consultation des instances représentatives du personnel, les salariés doivent être informés, préalablement des transferts de données envisagés à destination d'un pays non membre de l'Union européenne.

Cette information doit être rédigée en français. Elle doit préciser :

- le ou les pays d'établissement du destinataire des données;
- la nature des données transférées, (ex : identité, salaire, CV…);
- la finalité du transfert envisagé, (ex : hébergement des données par une société étrangère, centralisation des données par la société mère à des fins statistiques…);
- la ou les catégories de destinataires des données (ex : le service informatique, personnes habilités du service ressource humaines…).

Voir modèle proposé en annexe

4. Comment déclarer les transferts internationaux de données ?

Lorsque le transfert de données concerne un pays de l'Union européenne, il n'a pas à être autorisé par la CNIL.

En cas de transfert de données en dehors de l'Union européenne, l'employeur doit le préciser sur le formulaire de déclaration et remplir une annexe « transfert ».

Il doit ainsi joindre au dossier les garanties de protection des données y afférentes : existence de clauses contractuelles types issues des directives européennes, ou de règles internes d'entreprises (BCR), adhésion au *safe harbor*.

Le transfert doit ensuite faire l'objet d'une autorisation par la CNIL, sauf dans certains cas bien spécifiques (par exemple, entreprise destinataire adhérente au *safe harbor*).

Fiche n° 6 – contrôle de l'utilisation d'internet et de la messagerie

Pour l'exercice de leur activité professionnelle, les salariés ont à leur disposition un poste de travail informatique qui peut être connecté à internet et doté d'une messagerie électronique. L'utilisation, sur les lieux de travail, de ces outils informatiques à des fins autres que professionnelles est généralement tolérée. Elle doit rester raisonnable et ne doit pas affecter la sécurité des réseaux ou la productivité de l'entreprise ou de l'administration concernée.

1. Le contrôle de l'utilisation d'internet

L'employeur peut fixer les conditions et limites de l'utilisation d'internet, lesquelles ne constituent pas, en soi, des atteintes à la vie privée des salariés.

Par exemple : L'employeur peut mettre en place des dispositifs de filtrage de sites non autorisés (sites à caractère pornographique, pédophile, d'incitation à la haine raciale, révisionnistes, etc.). Il peut également fixer des limites dictées par l'exigence de sécurité de l'organisme, telles que l'interdiction de télécharger des logiciels, l'interdiction de se connecter à un forum ou d'utiliser le « chat », l'interdiction d'accéder à une boîte aux lettres personnelle par internet compte tenu des risques de virus qu'un tel accès est susceptible de présenter, etc.

> Nécessité d'informer les salariés
Les salariés doivent être informés des dispositifs mis en place et des modalités de contrôle de l'utilisation d'internet :

- Le comité d'entreprise doit avoir été consulté et informé (article L2323-32 du code du travail);
- Les salariés doivent être informés, notamment de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées.

Une durée de conservation de l'ordre de **six mois** est suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet.

Si des procédures disciplinaires sont susceptibles d'être engagées sur la base de ces fichiers, les salariés doivent en être explicitement informés (par exemple au moyen d'une charte).

> Comment déclarer?
Lorsque l'entreprise ou l'administration met en place un **dispositif de contrôle individuel des salariés destiné à produire un relevé des connexions ou des sites visités, poste par poste,** le traitement ainsi mis en œuvre doit être déclaré à la CNIL (déclaration normale) sauf si un correspondant informatique et libertés a été désigné, auquel cas aucune déclaration n'est nécessaire.

Par exemple : logiciel de contrôle de l'utilisation d'internet permettant d'analyser les données de connexion de chaque salarié ou de calculer le temps passé sur internet par un salarié déterminé.

Lorsque l'entreprise ou l'administration met en place un dispositif qui ne permet pas de contrôler individuellement l'activité des salariés, ce dispositif peut faire l'objet d'une déclaration de conformité en référence à la norme simplifiée n° 46 (gestion des personnels des organismes publics et privés).

Par exemple : logiciel permettant seulement de réaliser des statistiques sur l'utilisation d'internet au niveau de l'ensemble des salariés de l'entreprise ou au niveau d'un service déterminé.

2. Le contrôle de l'utilisation de la messagerie

Des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau peuvent conduire les entreprises ou les administrations à mettre en place des outils de contrôle de la messagerie.

Par exemple : outils de mesure de la fréquence, de la taille, des messages électroniques ; outils d'analyse des pièces jointes (détection des virus, filtres « anti-spam » destinés à réduire les messages non-sollicités, etc.).

> Nécessité d'informer les salariés
Les dispositifs de contrôle de la messagerie doivent faire l'objet d'une consultation du comité d'entreprise ou, dans la fonction publique, du comité technique paritaire ou de toute instance équivalente et d'une information individuelle des salariés.

Ils doivent notamment être informés, de la finalité du dispositif et de la durée pendant laquelle les données de connexion sont conservées ou sauvegardées.
En cas d'archivage automatique des messages électroniques, ils doivent en outre être informés des modalités de l'archivage, de la durée de conservation des messages, et des modalités d'exercice de leur droit d'accès.

> Comment déclarer ?
La messagerie professionnelle doit faire l'objet d'une déclaration de conformité en référence à la norme n° 46 (gestion des personnels des organismes publics et privés).

Si un **dispositif de contrôle individuel de la messagerie** est mis en place, il doit être déclaré à la CNIL (déclaration normale), sauf désignation d'un correspondant informatique et libertés.

Par exemple : logiciel d'analyse du contenu des messages électroniques entrant ou sortants destinés au contrôle de l'activité des salariés.

3. L'accès au poste informatique ou à la messagerie

> L'employeur doit respecter le secret des correspondances privées
Une communication électronique émise ou reçue par un employé peut avoir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles L.226-15 (pour le secteur privé) et L.432-9 (pour le secteur public) du Code pénal.

La Cour de cassation a affirmé, dans un arrêt du 2 octobre 2001 (arrêt « Nikon »), qu'un employeur ne saurait prendre connaissance de messages personnels d'un employé sans porter atteinte à la vie privée de celui-ci (article 9 du code civil) et au principe du secret des correspondances (article 226-15 du code pénal), quand bien même une utilisation à des fins privées aurait été proscrite par l'employeur.

Pour autant, le principe du secret des correspondances connaît des limites dans la sphère professionnelle. Il peut également être levé dans le cadre d'une instruction pénale ou par une décision de justice.

> Tout ce qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'employeur peut y accéder librement
La Cour de cassation considère qu'un message envoyé ou reçu depuis le poste de travail mis à disposition par l'employeur revêt un caractère professionnel, sauf s'il est identifié comme étant « personnel », dans l'objet du message par exemple (Cour de cassation, 30 mai 2007).

Il appartient à l'employé d'identifier les messages qui sont personnels. À défaut d'une telle identification, les messages sont présumés être professionnels.

La nature personnelle d'un message peut figurer dans l'objet du message ou dans le nom du répertoire dans lequel il est stocké.

La CNIL recommande de porter à la connaissance des salariés (par exemple dans une charte) le principe retenu pour différencier les e-mails professionnels des e-mails personnels (qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé, etc.).

> Le cas des fichiers et des répertoires créés par un employé
Il a été jugé que les fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel (Cour de cassation, 18 octobre 2006).

Tout fichier qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'employeur peut y accéder hors la présence du salarié.

En revanche, si un fichier est identifié comme étant personnel, l'employeur ne peut y avoir accès « qu'en présence du salarié ou si celui-ci a été dûment appelé, ou en cas de risque ou événement particulier ».

Par exemple : il a été jugé que la découverte de photos érotiques dans le tiroir d'un salarié ne constituait pas un risque ou un événement particulier justifiant que l'employeur accède au répertoire intitulé « perso » hors la présence du salarié ou sans que celui-ci en soit informé.

> L'employé doit exécuter son contrat de travail de bonne foi

L'employé ne doit pas transformer des messages de nature professionnelle en correspondance « privée ».

Par exemple : Un employé ne doit pas communiquer des documents confidentiels à un concurrent en identifiant ses messages comme étant « personnels ». Une telle identification serait contraire au principe de bonne foi prévu à l'article L1222-1 du Code du travail.

La Cour de cassation a ainsi admis, après avoir constaté que l'employeur avait des motifs légitimes de suspecter des actes de concurrence déloyale, qu'un employeur puisse être autorisé par le juge à mandater un huissier de justice pour prendre connaissance et enregistrer des messages électroniques échangés entre le salarié et deux personnes étrangères à l'entreprise (Cour de cassation, 23 mai 2007).

> L'employé est-il tenu de communiquer ses mots de passe ?

Si un employé est absent, l'employeur peut lui demander de communiquer son mot de passe lorsque les informations détenues par cet employé sont nécessaires à la poursuite de l'activité de l'entreprise (Cour de cassation, 18 mars 2003). L'employeur ne doit pas accéder au contenu personnel de l'intéressé.

La CNIL recommande que les modalités d'accès de l'employeur aux données stockées sur l'environnement informatique d'un employé absent soient préalablement définies en concertation et diffusées auprès de l'ensemble des salariés susceptibles d'être concernés (via une charte par exemple).

> Comment organiser la fermeture du compte utilisateur lors du départ de l'employé ?

Les modalités de fermeture du compte sont à prévoir dans la charte informatique. Il est recommandé à l'employeur d'avertir le salarié de la date de fermeture de son compte afin que ce dernier puisse vider son espace privé.

> Que faire en cas de difficulté ?

En cas de contestation, il appartient aux juridictions compétentes d'apprécier la régularité et la proportionnalité de l'accès par l'employeur au poste informatique ou à la messagerie de l'employé.

Fiche n° 7 – les administrateurs réseau

Les administrateurs ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Ils sont conduits par leurs fonctions même à avoir accès à des informations personnelles relatives aux utilisateurs (messagerie, historique des sites visités, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…).

> Accès aux données personnelles des utilisateurs

L'accès aux données enregistrées par les employés dans leur environnement informatique - qui sont parfois de nature personnelle - ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs.

De même, les administrateurs de réseaux et systèmes ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.

L'obligation de confidentialité pesant sur les administrateurs informatiques doit ainsi être clairement rappelée dans leur contrat, ainsi que dans la charte d'utilisation des outils informatiques annexée au règlement intérieur de l'entreprise ou de l'administration.

> L'utilisation des logiciels de prise de main à distance

Les logiciels de prise de main à distance peuvent notamment permettre aux gestionnaires techniques d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique.

Or, la CNIL constate parfois que ces outils de télémaintenance ou de prise de main à distance sont également utilisés à des fins de contrôle, par l'employeur, de l'activité de ses employés sur leur poste informatique. Une telle utilisation n'est ni conforme au principe de proportionnalité, ni respectueuse du principe de finalité posé par la loi « informatique et libertés ».

Dans l'hypothèse d'un recours à ces outils à des fins de maintenance informatique par un administrateur technique, leur utilisation doit s'entourer de précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquelles le gestionnaire technique accédera par ce moyen, dans la stricte limite de ses besoins.

Doivent notamment figurer au titre de ces précautions :

- l'information préalable et le recueil de l'accord de l'utilisateur pour « donner la main » à l'administrateur informatique avant l'intervention sur son poste (à titre d'illustration, l'accord peut être donné par simple validation d'un message d'information apparaissant sur son écran);
- la traçabilité des opérations de maintenance (par exemple, par la tenue d'un registre des interventions), ainsi que la précision dans les contrats des personnes assurant la maintenance - notamment en cas de recours à des prestataires extérieurs - de leur obligation de n'accéder qu'aux données informatiques nécessaires à l'accomplissement de leurs missions et d'en assurer la confidentialité.

L'utilisation de ces logiciels à des fins strictes de maintenance informatique n'est pas soumise à déclaration auprès de la CNIL.

Fiche n° 8 – la vidéosurveillance sur les lieux de travail

L'état actuel du droit se caractérise par la concurrence de deux régimes juridiques applicables : celui de la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004 et celui de l'article 10 de la loi du 21 janvier 1995 modifiée d'orientation et de programmation pour la sécurité (autorisation préfectorale).

Ceci explique le caractère complexe du régime juridique applicable en matière de vidéosurveillance.

Pour savoir quelle formalité préalable est nécessaire, il convient d'abord de déterminer si le dispositif de vidéosurveillance concerne un lieu public (ou ouvert au public) ou un lieu privé (ou non ouvert au public).

Distinction lieu public/lieu privé

- **lieu public ou ouvert au public : tout lieu du secteur public ou du secteur privé où le public peut accéder. *Exemple : le guichet d'une mairie ou un supermarché.***
- **lieu privé (lieu non ouvert au public) : tout lieu du secteur public ou du secteur privé où le public ne peut pas accéder. *Exemple : la chaîne de montage d'une entreprise automobile, le parking réservé au personnel d'une entreprise, un entrepôt ou des bureaux fermés au public***

Le régime juridique est clair dans deux cas :

- **Premier cas** : seule une autorisation préfectorale est nécessaire, quand le dispositif de vidéosurveillance est installé dans un lieu public ou ouvert au public et qu'aucune image n'est enregistrée ni conservée dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques ;
- **Deuxième cas** : seule une déclaration auprès de la CNIL est nécessaire, quand le dispositif est installé dans un lieu privé ou non ouvert au public et que les images sont enregistrées ou conservées dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques.

Le régime juridique n'est pas clair et pose problème lorsque le dispositif de vidéosurveillance est installé dans un lieu mixte (lieu ouvert au public qui comporte également des zones privées, par exemple un supermarché) et les images enregistrées dans un fichier ou traitées informatiquement. Dans cette hypothèses une déclaration auprès de la CNIL est nécessaire. Se pose toutefois la question du cumul avec la loi de 1995 (autorisation préfectorale).



Ce qu'il faut retenir :

Lorsque le dispositif d'enregistrement vidéo fait appel à des moyens informatiques (ex : surveillance vidéo IP, stockage des images sur support numérique, etc.) il est nécessaire de déclarer le dispositif à la CNIL.

Lorsque le système s'accompagne d'un dispositif biométrique (ex : reconnaissance faciale, analyse comportementale), Il doit faire l'objet d'une demande d'autorisation auprès de la CNIL puisqu'il fait appel à une technique biométrique (voir fiche n° 12).

2. La nécessité d'une analyse préalable des risques

Une réflexion préalable à l'installation d'un système de vidéosurveillance, basée sur une analyse précise des risques doit être menée afin d'identifier des solutions alternatives (une sécurisation des accès au moyen de badges magnétiques peut par exemple constituer la réponse efficace et adaptée à un objectif particulier de sécurisation).

3. La nécessité de respecter le principe de proportionnalité

La mise en œuvre d'un système de vidéosurveillance des employés doit nécessairement respecter le principe de proportionnalité. Elle doit donc s'effectuer de façon **adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi**.

Si le déploiement de tels dispositifs sur un lieu de travail répond généralement à un objectif sécuritaire (contrôle des accès aux locaux, surveillance de zones de travail à risques), il ne peut ainsi avoir pour seul objectif la mise sous surveillance spécifique d'un employé déterminé ou d'un groupe particulier d'employés.

Le nombre, l'emplacement, l'orientation, les fonctionnalités et les périodes de fonctionnement des caméras, ou la nature des tâches accomplies par les personnes devant être soumises à la vidéosurveillance, sont autant d'éléments à prendre en compte lors de l'installation du système.

L'enregistrement du son associé aux images rend le système encore plus intrusif. Dès lors, ce type d'enregistrements est disproportionné, sauf justification particulière.

Exemples de systèmes de vidéosurveillance susceptibles de présenter un caractère illégal : installation de caméras dans les vestiaires, les douches, les toilettes; installation d'un dispositif à l'insu des employés ou de façon non visible (caméra miniaturisée); système permettant d'enregistrer de façon spécifique les allées et venues des personnes se rendant dans un local syndical.

4. L'obligation d'information : pas de surveillance à l'insu des personnes

> l'information des salariés et visiteurs

Les personnes concernées (employés ou visiteurs) doivent être informées, au moyen d'un panneau affiché de façon visible dans les locaux sous vidéosurveillance, de l'existence du dispositif, des destinataires des images, ainsi que des modalités concrètes d'exercice de leur droit d'accès aux enregistrements visuels les concernant (voir modèle proposé en annexe).

> une consultation des représentants du personnel

Les instances représentatives du personnel doivent être consultées avant toute mise en œuvre d'un système de vidéosurveillance et précisément informées des fonctionnalités envisagées (article L2323-32 du code du travail, textes relatifs aux trois fonctions publiques, lois n° 84-16 du 11 janvier 1984, n° 84-53 du 26 janvier 1984 et n° 86-33 du 9 janvier 1986).

5. Une visualisation des images restreinte aux seuls destinataires habilités

Les images enregistrées ne peuvent être visionnées que par les seules personnes habilitées à cet effet, dans le cadre de leurs fonctions (par exemple : le responsable de la sécurité de l'organisme). Ces personnes doivent être particulièrement formées et sensibilisées aux règles encadrant la mise en œuvre d'un système de vidéosurveillance.

6. Une durée de conservation des images limitée

Les images ne devraient pas être conservées plus de quelques jours : en effet, en cas d'incident, la visualisation des images s'effectue généralement rapidement. Leur durée de conservation ne doit en tout état de cause s'étendre au-delà **d'un mois**.

Lorsque c'est techniquement possible, une durée maximale de conservation des images doit être paramétrée dans le système. Elle ne doit pas être fixée en fonction de la capacité technique de stockage de l'enregistreur.

7. Comment déclarer ?

Un système de vidéosurveillance numérique mis en place sur un lieu de travail ne peut être installé que s'il a préalablement fait l'objet d'une déclaration normale auprès de la CNIL, sauf désignation d'un correspondant informatique et libertés.

Un système qui n'aurait pas fait l'objet d'une déclaration à la CNIL ne peut être opposé aux employés.

Fiche n° 9 – la gestion de la téléphonie

I- L'utilisation du téléphone au travail

La possibilité d'un usage personnel du téléphone est reconnue à condition qu'une telle utilisation demeure raisonnable et ne soit pas préjudiciable à l'employeur. Il est ainsi légitime qu'un employeur s'assure du caractère non abusif de cette utilisation. Ce contrôle doit toutefois s'opérer dans des conditions propres à garantir le respect de la vie privée et des libertés des personnels sur leur lieu de travail.

1. La mise en place des autocommutateurs

Les autocommutateurs sont des standards téléphoniques permettant d'orienter l'ensemble des numéros de téléphone appelants et des numéros appelés. Ces appareils permettent même l'enregistrement des numéros de téléphone sortants, de sorte que ces dispositifs sont susceptibles d'être utilisés afin d'identifier les communications téléphoniques qui relèveraient d'un usage non professionnel.

Ils peuvent également servir à la comptabilisation statistique des flux entrants et sortants au niveau de l'organisation, d'un service ou d'un poste particulier. Reliés à des logiciels « de taxation », ils peuvent permettre d'imputer et de contrôler par service ou par poste les dépenses téléphoniques de l'organisation.

2. La gestion des relevés téléphoniques

Lorsque des relevés sont établis (ex : facturation détaillée des opérateurs de téléphone), **les quatre derniers chiffres de ces numéros doivent être occultés.**

Les supérieurs hiérarchiques ne doivent accéder aux numéros complets des relevés individuels que de façon exceptionnelle (par exemple en cas d'utilisation manifestement anormale du téléphone par un salarié).

Bien entendu, un salarié doit avoir la possibilité d'accéder aux numéros de téléphone complets composés depuis son poste téléphonique, notamment lorsqu'il lui est demandé le remboursement du coût des communications téléphoniques présumées personnelles.

La durée de conservation des données relatives à l'utilisation des services de téléphonie ne doit pas excéder un an.

3. Les droits spécifiques des employés protégés

Toute utilisation des informations issues de l'utilisation des services de téléphonie pour un contrôle des appels émis et reçus par les représentants du personnel et les représentants syndicaux dans le cadre de leur mandat est **interdite**.

Depuis un arrêt de la Cour de Cassation du 6 avril 2004, les employés investis d'un mandat électif ou syndical doivent pouvoir disposer d'un matériel excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants (par exemple via une ligne non connectée à l'autocommutateur ou ne pouvant donner lieu à la production d'une facturation détaillée).

4. Comment déclarer ?

Concernant les fichiers mis en œuvre dans le cadre de l'utilisation de service de téléphonie fixe et mobile, l'employeur a la possibilité d'effectuer une déclaration de conformité à la norme simplifiée n°47.

Si toutefois, le dispositif mis en place dépasse le cadre prévu par cette norme, l'employeur doit faire une déclaration normale sauf en cas de désignation d'un correspondant informatique et libertés (dispense de déclaration).

II – L'enregistrement des conversations téléphoniques sur le lieu de travail

L'enregistrement des conversations téléphoniques ne peut être réalisé qu'en cas de nécessité reconnue et doit être proportionné aux objectifs poursuivis.

Par exemple, un enregistrement pour des besoins de formation ne pourra être réalisé que sur une brève période et en aucun cas de manière permanente.

1. Quelles garanties pour les salariés ?

> Neutralisation de la fonction enregistrement pour les appels privés
En cas d'enregistrement des communications téléphoniques, il convient que les employés disposent de lignes téléphoniques non reliées au système d'enregistrement ou d'un dispositif technique leur permettant, en cas de conversation privée, de se mettre hors du champ du dispositif d'enregistrement, tant pour les appels entrants que sortants (par exemple : possibilité d'utiliser une touche particulière avant de composer un numéro de téléphone pour neutraliser la fonction d'enregistrement).
Ces fonctionnalités doivent être offertes tout particulièrement dans le cas des salariés protégés (représentants du personnel ou syndicaux).

> Information des salariés
Outre la consultation des instances représentatives du personnel, les salariés ainsi que leurs interlocuteurs, doivent être informés, préalablement à la mise en place du dispositif :

- des objectifs poursuivis par l'installation de ce système;
- des conséquences individuelles qui pourront en résulter;
- des destinataires des enregistrements;
- des modalités d'exercice de leur droit d'accès.

L'information des interlocuteurs peut notamment être réalisée par la diffusion d'un message au début de l'appel, ou par l'insertion d'une mention particulière dans le document contractuel ou d'information relatif au service téléphonique (voir modèle proposé en annexe.)

Dans le cadre d'enregistrements ou d'écoutes à des fins de formation ou d'évaluation, les salariés doivent être informés des périodes pendant lesquelles leurs conversations sont susceptibles d'être enregistrées ou écoutées.

Si des procédures disciplinaires sont susceptibles d'être engagées sur la base des enregistrements ou des comptes rendus, les salariés doivent en être explicitement informés.

Attention
Les principes exposés ci-dessus sont également applicables en cas d'écoute des conversations téléphoniques sans enregistrement.

2. Combien de temps l'employeur peut-il garder les enregistrements ?

Lorsque les enregistrements sont réalisés à des fins de formation du personnel, la Commission recommande une durée de conservation maximale de 6 mois.

Lorsque les enregistrements sont réalisés à des fins de preuve en matière bancaire, la durée de conservation doit être conforme aux articles 321-78 et 321-79 du Règlement Général de l'Autorité des Marchés Financiers (cinq ans maximum).

En matière d'écoutes téléphoniques, la Commission recommande que les comptes rendus des conversations téléphoniques et grilles d'analyse soient conservés pour une durée d'un an maximum.

3. Comment déclarer ?

L'enregistrement des conversations téléphoniques doit faire l'objet d'une déclaration normale auprès de la CNIL si le dispositif d'enregistrement repose sur des moyens numériques.

L'écoute des conversations téléphoniques doit faire l'objet d'une déclaration normale auprès de la CNIL si elle est suivie d'un compte rendu ou d'une grille d'analyse.

En cas de désignation d'un correspondant informatique et libertés, aucune déclaration n'est nécessaire.

Fiche n° 10 – les dispositifs de géolocalisation gsm/gps

Certains employeurs équipent leurs véhicules professionnels de dispositifs de géolocalisation GPS/GSM. Compte tenu des risques d'atteinte aux droits et libertés des personnes que comporte l'utilisation de ces dispositifs, la CNIL a estimé nécessaire de préciser, dans une recommandation du 16 mars 2006, les conditions dans lesquelles ils pouvaient être utilisés.

1. Pourquoi géolocaliser les véhicules des employés ?

Un dispositif de géolocalisation peut être mis en place pour les finalités suivantes à savoir :

- la contribution à la sécurité des personnes ou des marchandises transportées ;
- une meilleure gestion des moyens en personnel et véhicules (prestations à accomplir en des lieux dispersés) ;
- le suivi et la facturation d'une prestation ;
- le suivi du temps de travail des employés, lorsque ce suivi ne peut être réalisé par d'autres moyens.

En revanche, le recours à la géolocalisation n'est pas justifié lorsqu'un employé dispose d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP, etc.).

L'utilisation d'un dispositif de géolocalisation ne doit pas conduire à un contrôle permanent de l'employé concerné. Ainsi, la CNIL recommande la désactivation du système embarqué dans les véhicules de fonction des employés en dehors des horaires de travail.

2. À quelles conditions ?

La mise en œuvre d'un traitement de géolocalisation :

- ne doit pas permettre la collecte d'informations concernant les éventuels dépassements des limitations de vitesse ;
- doit nécessairement s'accompagner de mesures de sécurité limitant l'accès aux données de géolocalisation aux personnes habilitées ;
- nécessite de fixer une durée de conservation adéquate de ces données (généralement 2 mois) ;
- implique au préalable la consultation des instances représentatives du personnel et l'information individuelle des employés concernés relative à la finalité du traitement, les données traitées, leur durée de conservation, les destinataires des données, leurs droits d'accès, de rectification et d'opposition (voir modèle proposé en annexe) ;
- ne doit pas s'appliquer aux employés investis d'un mandat électif ou syndical lorsqu'ils agissent dans le cadre de leur mandat.

3. Comment déclarer ?

Si le dispositif de géolocalisation des véhicules des employés est en tout point conforme aux prescriptions de la norme simplifiée n° 51 du 16 mars 2006, le responsable du traitement peut procéder en ligne à une déclaration de conformité à cette norme. Dans les autres cas, il lui appartiendra d'adresser une déclaration normale à la CNIL, sauf désignation d'un Correspondant informatique et libertés (dispense de déclaration).

Fiche n° 11 – utilisation de badges sur le lieu de travail

Sur le lieu de travail, les badges électroniques (cartes magnétiques ou à puce) servent notamment au contrôle des accès aux locaux, à la gestion des temps de travail, ainsi qu'à la gestion de la restauration d'entreprise.

Ces différents types de dispositifs, qui comportent des données permettant l'identification des employés, sont soumis à la loi « informatique et libertés » et, ainsi que la Cour de cassation l'a rappelé dans son arrêt du 6 avril 2004, doivent être préalablement déclarés auprès de la CNIL, sauf désignation d'un correspondant informatique et libertés.

1. Quelles garanties prévoir ?

Chaque passage du badge dans un lecteur permet l'enregistrement de données relatives à son détenteur. Ces enregistrements présentent des risques d'utilisation détournée et sont notamment susceptibles de « tracer » les déplacements des salariés à des fins de surveillance de leur activité.

Par ailleurs, les enregistrements réalisés peuvent parfois permettre à l'employeur d'accéder à des informations privées (consommations de ses personnels au sein du restaurant d'entreprise).

Des garanties particulières doivent donc être apportées par l'employeur pour éviter de tels détournements de finalité. Il doit notamment préciser :

- la finalité du dispositif (ex : contrôle des accès, gestion des temps de présence…);
- les informations qui seront collectées;
- les services destinataires des données;
- les modalités d'exercice du droit d'accès à ces données.

Les personnels et leurs représentants doivent être parfaitement informés de ces modalités, préalablement à la mise en œuvre du système de badges (voir modèle proposé en annexe).

2. Comment déclarer ?

Si le dispositif envisagé respecte en tout point le cadre fixé par la norme simplifiée n° 42, l'employeur privé ou public peut effectuer une déclaration simplifiée sauf s'il a désigné un correspondant informatique et libertés auquel cas il est dispensé de déclaration.

Dans le cas contraire - notamment en cas de recours à des dispositifs biométriques -, des formalités de déclaration particulières voire de demande d'autorisation devront être accomplies auprès de la CNIL (cf. fiche n°12).

Fiche n° 12 – la biométrie sur le lieu de travail

Les dispositifs biométriques, parce qu'ils permettent d'identifier une personne par ses caractéristiques physiques, biologiques voire comportementales, sont particulièrement sensibles et sont donc soumis à un contrôle particulier de la CNIL.

Ainsi, ces dispositifs ne peuvent être mis en œuvre sans autorisation préalable de la CNIL.

La biométrie, qu'est-ce que c'est ?

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales…). Elles se rapprochent ainsi de ce qui pourrait être défini comme un « identificateur unique universel », permettant de fait le traçage des individus.

1. Le cadre juridique

Tous les dispositifs de reconnaissance biométrique sont soumis à autorisation préalable de la CNIL quel que soit le procédé technique retenu (contour ou forme de la main, empreinte digitale…). Il appartient à chaque organisme d'adresser une demande d'autorisation à la CNIL. Sauf trois cas de figure précisés ci-après, chaque application fait l'objet d'un examen au cas par cas, en fonction notamment de la caractéristique biométrique utilisée.

Attention

La CNIL n'agrée pas et ne labellise pas les dispositifs biométriques. Les sociétés qui commercialisent ce type de dispositifs ne peuvent donc en aucune façon se prévaloir d'un quelconque agrément de la CNIL sur leur produit.

2. Des formalités allégées pour certains dispositifs biométriques

Afin de faciliter les formalités, la Commission a défini un cadre, appelé autorisation unique, applicable à certains dispositifs biométriques. Le principe est le suivant : lorsque, par exemple, un employeur souhaite mettre en œuvre un dispositif biométrique qui répond aux conditions définies dans ce cadre, il peut bénéficier d'une procédure simplifiée. Il lui suffit alors d'adresser à la CNIL une simple déclaration de conformité.



Cette procédure d'autorisation unique s'applique à trois types de dispositifs reposant sur la reconnaissance :

- du contour de la main pour assurer le contrôle d'accès au restaurant scolaire (autorisation n°AU-009);
- du contour de la main pour assurer le contrôle d'accès et la gestion des horaires et de la restauration sur les lieux de travail (autorisation n°AU-008);
- de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels (autorisation n°AU-007).

Attention
L'utilisation de dispositifs de reconnaissance biométrique, pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration ne peut être déclarée en référence à la norme simplifiée n° 42, relative aux traitements de contrôle d'accès.

3. La nécessaire information préalable des intéressés

Les personnes concernées par le dispositif biométrique doivent être clairement informées de ses conditions d'utilisation, de son caractère obligatoire ou facultatif, des destinataires des informations et des modalités d'exercice de leurs droits d'opposition, d'accès et de rectification. En outre, et conformément au Code du travail et à la législation applicable à la fonction publique territoriale, les instances représentatives du personnel doivent, le cas échéant, être consultées et informées avant la mise en œuvre des dispositifs.

voir modèle proposé en annexe

4. Le cas particulier des dispositifs reposant sur l'enregistrement des empreintes digitales dans une base de données

Dans une communication destinée à mieux informer les salariés sur leurs droits et permettre aux entreprises et administrations de se poser les bonnes questions « informatique et libertés » la CNIL rappelle que :

- **l'empreinte digitale est une biométrie à « trace ».** Chacun laisse des traces de ses empreintes digitales, plus ou moins facilement exploitables, dans beaucoup de circonstances de la vie courante (sur un verre ou une poignée de porte etc.) ;

- **ces « traces » peuvent être capturées à l'insu des personnes et être utilisées notamment pour usurper leur identité.**

Par conséquent, ces dispositifs ne sont justifiés que s'ils sont fondés sur un fort impératif de sécurité et satisfont aux quatre exigences suivantes :

- **la finalité du dispositif :** elle doit être limitée au contrôle de l'accès d'un nombre limité de personnes à une zone bien déterminée, représentant ou contenant un enjeu majeur dépassant l'intérêt strict de l'organisme tel que la protection de l'intégrité physique des personnes, de celle des biens et des installations ou encore de celles de certaines informations (ex : accès à une centrale nucléaire, à une cellule de production de vaccins ou à un site Seveso II) ;
- **la proportionnalité :** le système proposé est-il bien adapté à la finalité préalablement définie eu égard aux risques qu'il comporte en matière de protection des données à caractère personnel ?
- **la sécurité :** le dispositif doit permettre à la fois une authentification et/ou une identification fiable des personnes et comporter toutes garanties de sécurité pour éviter la divulgation des données ;
- **l'information des personnes concernées :** elle doit être réalisée dans le respect de la loi « informatique et libertés » et, le cas échéant, du Code du travail.

5. Comment déclarer ?

Si le dispositif biométrique est conforme à l'une de ces trois autorisations uniques, il suffit d'adresser à la CNIL une simple déclaration de conformité qui peut s'effectuer en ligne sur www.cnil.fr.

Les traitements ne relevant pas de l'une de ces autorisations uniques doivent faire l'objet d'une demande d'autorisation. Cette demande est constituée du formulaire de déclaration, complété et signé par le responsable du traitement ou son représentant, accompagné des annexes « sécurité » (également disponibles sur le site web de la CNIL), ainsi que de tout élément justifiant la mise en place du dispositif de reconnaissance biométrique envisagé.

Mode d'emploi : comment déclarer ?

La déclaration est une obligation légale dont le non-respect est pénalement sanctionné[1]. Tout fichier ou traitement informatisé comportant des données personnelles doit donc être déclaré à la CNIL préalablement à sa mise en œuvre, sauf s'il est expressément exonéré de déclaration. Cette formalité peut prendre plusieurs formes selon le fichier concerné (voir tableau récapitulatif à la fin du guide.).

Les déclarations peuvent être réalisées en ligne sur le site de la CNIL (www.cnil.fr rubrique « déclarer »). En cas de doute sur le régime dont relève le traitement, il suffit de réaliser une déclaration normale en ligne : la CNIL se chargera de qualifier le dossier et de contacter le déclarant.

Dans tous les cas, la désignation d'un correspondant « informatique et libertés » (CIL) dispense l'organisme concerné de devoir accomplir les formalités relatives aux fichiers relevant de la déclaration simplifiée et de la déclaration normale. Le formulaire de désignation d'un CIL est accessible sur le site www.cnil.fr.

1. Les dispenses de déclaration

Un certain nombre de traitements, décrits dans le tableau récapitulatif figurant ci-après, sont dispensés de déclaration par une décision de la CNIL (paie du personnel, comptabilité…).

Attention

Le fait d'être exonéré ne signifie pas pour autant que vous n'avez aucune obligation. Vous devez notamment garantir le droit d'information des personnes ainsi que la sécurité des données (voir modèles proposés en annexe)

2. La déclaration simplifiée

La plupart des fichiers des entreprises ou administrations peuvent faire l'objet de **déclarations simplifiées**, qui se font en ligne sur le site de la CNIL (www.cnil.fr, rubrique « Déclarer »).

3. La déclaration normale

Le régime de droit commun est la **déclaration normale**, lorsque le fichier ne relève pas d'une procédure particulière (art. 22 de la loi du 6 janvier 1978 modifiée en 2004). Le traitement peut être mis en œuvre dès réception du récépissé délivré par la CNIL.

Le récépissé atteste de l'accomplissement des formalités de déclaration, mais n'exonère pas le responsable du respect des autres obligations

[1] Article 226-16 du code pénal : « Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

prévues par la loi (en ce qui concerne la finalité du fichier, sécurité et confidentialité, les droits des personnes…).

4. Les formalités particulières

Certains traitements peuvent relever d'un **régime d'autorisation** ou de **demande d'avis**. Il s'agit de régimes plus protecteurs, qui s'appliquent aux fichiers considérés comme « sensibles » ou comportant des risques pour la vie privée ou les libertés.

> La procédure d'autorisation (art. 25) concerne :
- les traitements qui comportent des données sensibles énumérées à l'article 8 de la loi ;
- les traitements qui comportent des données relatives aux infractions ou condamnations ;
- les traitements qui comportent le numéro de sécurité sociale (NIR) ou qui nécessitent une interrogation du répertoire national d'identification des personnes physiques (RNIPP) ;
- les traitements qui procèdent à l'interconnexion de fichiers dont les finalités principales sont différentes ;
- les traitements de données comportant des appréciations sur les difficultés sociales des personnes ;
- les traitements qui utilisent des données biométriques.

Le traitement devra respecter en tout point le cadre fixé par l'autorisation délivrée par la CNIL.

> La procédure de demande d'avis (art. 27) concerne principalement les administrations ou les entreprises gérant un service public pour les fichiers comportant le numéro de sécurité sociale (NIR) ou nécessitant une interrogation du répertoire national d'identification des personnes physiques (RNIPP), et les téléservices de l'administration électronique comportant un identifiant des personnes physiques.

La demande d'avis doit être accompagnée d'un projet d'arrêté ou de décision de l'organe délibérant, destiné à autoriser le traitement une fois l'avis de la CNIL rendu.

5. Une fois le dossier complété

Dans le cas d'une **déclaration en ligne**, la CNIL adresse immédiatement après envoi un accusé de réception électronique.

La CNIL délivre ensuite par voie postale ou électronique un **récépissé de déclaration** indiquant le numéro sous lequel le traitement déclaré est enregistré.

Pour les procédures particulières d'autorisation ou d'avis, la CNIL adresse au déclarant une notification de l'autorisation ou de l'avis qu'elle a rendu.

Tableau récapitulatif : quelle déclaration pour quel fichier ?

FINALITÉ DU FICHIER	FORMALITÉS DÉCLARATIVES	CONDITIONS PARTICULIÈRES
Paie Déclarations fiscales et sociales obligatoires (déclarations aux organismes de protection sociale, de retraite et de prévoyance, DADS, DUE, travailleurs handicapés…), y compris celles réalisées à partir de www.net-entreprises.fr Tenue des registres obligatoires (registre unique du personnel…) Tenue des comptes individuels relatifs à l'intéressement et à la participation Statistiques non nominatives liées à l'activité salariée dans l'entreprise	**AUCUNE**	Respecter les termes de la **dispense n° 1** (employeurs publics) ou la **dispense n° 2** (employeurs privés) du 9 décembre 2004 **Attention :** Les transferts de données vers un pays tiers à l'Union Européenne ne sont pas dispensés.
Tenue d'une liste d'initiés dans les conditions fixées par le Code des marchés financiers	**AUCUNE**	Respecter les termes de la **dispense n°9** du 6 juillet 2006
Comptabilité générale	**AUCUNE**	Respecter les termes de la **dispense n° 80-34** du 21 octobre 1980
Traitements mis en œuvre par les CE, ou les délégués du personnel pour la gestion de leurs activités sociales et culturelles	**AUCUNE**	Respecter les termes de la **dispense n° 10** du 17 octobre 2006
• Gestion des contrôles d'accès aux locaux, • Gestion des horaires, • Gestion de la restauration d'entreprise	**DÉCLARATION SIMPLIFIÉE** Si désignation d'un correspondant informatique et libertés : **AUCUNE**	Respecter la **norme simplifiée n° 42**. Cette norme ne concerne pas les traitements recourant à un procédé de reconnaissance biométrique, qui sont soumis à une procédure d'autorisation

Fichiers courants de gestion des ressources humaines : • gestion administrative (dossiers professionnels, annuaires, élections professionnelles, convocations) • mise à disposition d'outils informatiques (suivi et maintenance, annuaires informatiques, messagerie électronique, Intranet) • organisation du travail (agenda professionnel, gestion des tâches) • gestion des carrières (évaluation, validation des acquis, mobilité…) • gestion de la formation	**DÉCLARATION SIMPLIFIÉE** Si désignation d'un correspondant informatique et libertés : **AUCUNE**	Respecter la **norme simplifiée n° 46**. Cette norme exclut notamment : • les traitements permettant le contrôle individuel de l'activité des employés • les dispositifs ayant pour objet l'établissement du profil psychologique des employés • les transferts de données vers un pays tiers à l'union européenne
Mise en œuvre de services de téléphonie fixe et mobile sur les lieux de travail Gestion des communications (annuaire interne, gestion des dotations, messagerie téléphonique interne, maîtrise des dépenses liées à l'utilisation des services de téléphonie…)	**DÉCLARATION SIMPLIFIÉE** Si désignation d'un correspondant informatique et libertés : **AUCUNE**	Respecter la **norme simplifiée n° 47**. Cette norme exclut expressément : • les finalités relatives à l'écoute ou à l'enregistrement de conversations téléphoniques • la localisation d'un employé à partir de son téléphone portable
Mise en œuvre de services destinés à géolocaliser les véhicules utilisés par les employés	**DÉCLARATION SIMPLIFIÉE** Si désignation d'un correspondant informatique et libertés : **AUCUNE**	Respecter la **norme simplifiée n° 51**.

Tout autre traitement automatisé, dès lors qu'il n'est pas conforme aux normes élaborées par la Commission, notamment : Annuaires du personnel sur internet Traitements informatiques permettant un contrôle de l'activité professionnelle des salariés (surveillance des connexions internet ou de la messagerie électronique, géolocalisation) Traitements de vidéosurveillance Traitements de recrutement (base de données de CV ou de candidats)	**DÉCLARATION NORMALE** Si désignation d'un correspondant informatique et libertés : **AUCUNE**	Utiliser le formulaire de déclaration normale (téléchargeable sur le site de la CNIL www.cnil.fr, rubrique déclarer, mode d'emploi) Pour les fichiers de recrutement : se référer à la recommandation n° 02-017 du 21 mars 2002
Traitements comportant un transfert de données vers un pays tiers à l'Union européenne	**AUTORISATION**	
Dispositifs biométriques : reconnaissance du contour de la main pour assurer le contrôle d'accès et la gestion des horaires et de la restauration sur les lieux de travail	**AUTORISATION UNIQUE**	Respecter les termes de l'autorisation unique **AU-008**
Dispositifs biométriques : reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels	**AUTORISATION UNIQUE**	Respecter les termes de l'autorisation unique **AU-007**
Dispositifs d'alerte professionnelle (lignes éthiques) dans le domaine financier, comptable, bancaire et de la lutte contre la corruption.	**AUTORISATION UNIQUE**	Respecter les termes de l'autorisation unique **AU-004**

Autres dispositifs biométriques	**AUTORISATION**	Un système recourant, par exemple, à un procédé de reconnaissance des empreintes digitales avec base centrale ne peut être mis en œuvre sans l'autorisation préalable de la CNIL
Autres dispositifs d'alertes professionnelles	**AUTORISATION**	Un dispositif permettant de signaler des violations autres que comptables ou financières (ex : harcèlement, atteinte aux droits de propriété intellectuelle, violation d'un code de bonne conduite…)

Dans tous les cas, la déclaration doit être effectuée avant la mise en œuvre du traitement. Cette mise en œuvre ne peut intervenir qu'à réception du récépissé de déclaration (pour les déclarations simplifiées et normales) ou de l'autorisation de la CNIL (pour les demandes d'autorisation).

Droit à l'information

Conformément aux dispositions du code du travail (L2323-32) et aux textes relatifs aux trois fonctions publiques (lois n°84-16 du 11 janvier 1984, n°84-53 du 26 janvier 1984 et n°86-33 du 9 janvier 1986), les instances représentatives du personnel doivent être consultées et précisément informées des fonctionnalités envisagées dans le cas de mise en œuvre de traitements qui ont une incidence sur le personnel.

De plus, le code du travail prévoit qu'aucune information concernant directement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance (L1221-9 et L1222-4).

Les employés doivent, **dans tous les cas de figure**, être informés **individuellement** de l'existence des traitements contenant des données personnelles les concernant par note, affichage, publication dans le journal interne, courrier électronique…

En application de la loi du 6 janvier 1978 modifiée, les personnels concernés doivent être informés de la ou des finalité(s) et fonctionnalités précises de chaque traitement automatisé mis en œuvre par l'employeur, des conséquences individuelles qui pourront en résulter (par exemple un contrôle), des destinataires des données enregistrées et de leur droit d'accès, d'opposition et de rectification à ces données.

À cet égard, la déclaration adressée à la CNIL doit préciser les mesures relatives à l'information individuelle des salariés.

Toute personne peut obtenir communication de la liste des traitements déclarés au sein d'un organisme sur simple demande écrite (article 31 de la loi du 6 janvier 1978 modifiée). Le contenu d'un dossier de déclaration peut être communiqué au titre de la loi dite « CADA » du 17 juillet 1978.

Exemples de notes d'informations

(Ces exemples doivent être adaptés par le responsable du traitement)

Mention d'information à porter sur les formulaires de collecte

.... *(indication de l'identité du responsable du traitement)* « Les informations recueillies font l'objet d'un traitement informatique destiné à … *(préciser la finalité)*. Les destinataires des données sont : .... *(précisez)*.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. que vous pouvez exercer en vous adressant à .... *(préciser le service et l'adresse)*. (vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant).

Note d'information susceptible d'être affichée

Le(s) service(s)......................................*(citer le nom du ou des services responsables du traitement)* dispose(nt) de moyens informatiques destinés à gérer plus facilement ....*(indiquer la finalité du traitement)*.

Les informations enregistrées sont réservées à l'usage du (ou des) service(s) concerné(s) et ne peuvent être communiquées qu'aux destinataires suivants : .... *(préciser les destinataires)*.

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service..*(citer le nom du service ou des services concernés)*.

Courrier d'information (annuaire diffusé sur internet)

Madame, Monsieur,

Nous envisageons de diffuser prochainement sur notre site Internet *(indiquez ici le nom de domaine de votre site. Exemple : www.monsite.fr)* des informations vous concernant dans le cadre de *(A compléter : Exemples : site internet d'une administration, d'une association, d'un groupement professionnel, d'une entreprise, etc.)*. Ces informations sont les suivantes : *(Indiquez ici les informations que vous allez diffuser. Exemples : nom, prénom, diplôme, etc.)*.

Compte tenu des caractéristiques du réseau Internet que sont la libre captation des informations diffusées et la difficulté, voire l'impossibilité de contrôler l'utilisation qui pourrait en être faite par des tiers, vous pouvez vous opposer à une telle diffusion. Pour que nous puissions prendre en compte votre refus, contactez-nous.

Attention!

En l'absence de réponse de votre part dans un délai d'un mois à compter de la réception de ce courrier, votre accord sera réputé acquis. Vous pourrez toutefois nous faire part ultérieurement, à tout moment, de votre souhait que la diffusion de vos données sur Internet cesse.

Nous vous rappelons que vous disposez d'un droit d'accès, de modification, de rectification et de suppression des données qui vous concernent. Pour exercer ce droit, adressez-vous à :

(indiquez ici l'adresse où les personnes peuvent exercer leur droit d'accès et de rectification)

Panneau d'information (videosurveillance)

(ce panneau doit être situé a l'entrée de l'établissement et visible par les salariés et les personnes extérieures)

Établissement sous vidéosurveillance
(représentation graphique d'une caméra)

Nous vous informons que cet établissement est placé sous vidéosurveillance pour des raisons de … *(indiquer les finalités poursuivies)*. Pour tout renseignement, s'adresser au service … ou à … *(identifier la personne ou le service compétent)*, auprès duquel vous pouvez également exercer votre droit d'accès, conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004.

Note d'information adressée au personnel (géolocalisation)

……………………………… *(indication de l'identité du responsable du traitement)* Nous avons installé, dans les véhicules, un système permettant de les localiser en temps réel.

Ce nouveau service va nous servir *(précisez ici la finalité, par exemple, repérer le véhicule le plus proche à la demande d'un client)*. Nous aurons connaissance de l'itinéraire que vous suivez ainsi que des arrêts que vous effectuez.

Les données relatives à vos déplacements sont conservées au maximum *(précisez)*. Au-delà, toutes les données sont rendues anonymes et ont pour seul objet la réalisation de statistiques.

Seuls les services suivants sont destinataires de ces informations (précisez, par exemple direction des ressources humaines, responsables opérationnels…).

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous pouvez avoir accès et rectifier les informations qui vous concernent en vous adressant à ……………………………… *(préciser le service et l'adresse)*.

Note d'information pour un dispositif de contrôle d'accès (badges, biométrie)

……………………………… *(indication de l'identité du responsable du traitement)*
Un dispositif (biométrique) destiné au contrôle de l'accès ……………………………… *(préciser ici la finalité, par exemple contrôle d'accès à un bâtiment ou à une zone en particulier, contrôle d'accès à un poste informatique ou à une application)* a été mis en place.

Les données vous concernant sont conservées au maximum *(précisez)*. Au-delà, toutes les données sont détruites.

Seules les personnes habilitées du service ……………………………… *(préciser le service – par exemple le service informatique)* auront accès à vos données biométriques.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous pouvez avoir accès et rectifier les informations qui vous concernent en vous adressant à ……………………………… *(préciser le service et l'adresse)*.

Information par message téléphonique (enregistrement téléphonique)

Nous vous informons que votre conversation téléphonique est susceptible d'être enregistrée pour des raisons de … *(indiquer les finalités poursuivies)*.
Vous pouvez vous opposez à cet enregistrement de la manière suivante : (préciser la procédure à suivre, appui sur une touche téléphonique, demande à formuler à l'opérateur…)
En cas d'enregistrement des conversations, ceux-ci son conservés pour une durée de (préciser la durée). Seules les personnes habilitées du service ……………………………… *(préciser le service – par exemple le service clientèle)* auront accès à cet enregistrement.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous pouvez accéder et rectifier les informations qui vous concernent en vous adressant à ……………………………… *(préciser le service et l'adresse)*.

Notice d'information en matière de recrutement

(à remettre au candidat)

……………………………….. *(indication de l'identité du responsable du traitement)*
Nous vous prions de bien vouloir compléter soigneusement ce formulaire. Les réponses aux cases munies d'un astérisque sont facultatives et sans conséquence pour l'examen du dossier; dans les autres cas, le défaut réponse est susceptible de compromettre le bon suivi de votre candidature.

Conformément au Code du travail, nous vous informons que la procédure de recrutement utilisée par notre société comprend : *(à préciser, par exemple des entretiens, éventuellement une analyse graphologique et/ou des tests psychotechniques). Dans ce dernier cas il convient d'ajouter :* Les résultats de ces tests vous seront restitués sur demande, ils ne seront conservés dans votre dossier qu'en cas d'embauche.

Nous vous informons que les données vous concernant sont (ou ne sont pas) informatisées, elles seront traitées de façon confidentielle. Vos données sont conservées pour une durée de *(à préciser, au maximum 24 mois à compter du dernier contact avec le candidat)*.

Seules les personnes habilitées de notre société pourront accéder à vos données à des fins strictement internes.

Option pour les groupes internationaux :

J'autorise la société à communiquer les informations me concernant aux filiales du groupe situées en dehors de l'Union Européenne : Oui ❏ Non ❏

Option pour les cabinets de recrutement :

J'autorise la société à communiquer les informations me concernant à toute entreprise cliente : Oui ❏ Non ❏

Option pour les « cvthèques » en ligne :

J'autorise la société à :

- communiquer les informations me concernant à toute entreprise cliente qui en ferait la demande : Oui ❏ Non ❏
- diffuser en ligne les informations me concernant sans les rendre anonymes : Oui ❏ Non ❏

Vous pouvez accéder aux informations vous concernant, les rectifier ou les supprimer pour ce faire il suffit de vous adresser auprès du service suivant : (à préciser).

Fait le .... à ....
Signature :

Mention d'information en cas de transfert de donnés en dehors de l'union européenne

……………………………………… *(identité du responsable du traitement)* dispose(nt) de moyens informatiques destinés à gérer ……………………… *(indiquer la finalité du traitement, par exemple la gestion des ressources humaines, le gestion de la paie, la maintenance informatique, etc.…).*

Les informations enregistrées sont réservées à l'usage du (ou des) service(s) concerné(s) et ne peuvent être communiquées qu'aux destinataires suivants : … *(préciser les destinataires)*.

Certains de ces destinataires sont situés en dehors de l'Union Européenne, et en particulier les destinataires suivants *(indiquer le nom des entités ou services destinataires ainsi que leur pays d'établissement)*

Ces destinataires auront communication des données suivantes *(à préciser, par exemple nom, prénom, matricule, coordonnées professionnelles, salaire, données de connexion…)*

La transmission de ces données aux destinataires situés en dehors de l'Union Européenne est destinée à ……………….. *(indiquer la finalité du transfert des données).*

Les garanties suivantes ont été prises pour s'assurer d'un niveau de protection suffisant des données personnelles :

- Le pays du ou des destinataires(s) offre un niveau de protection adéquat par décision de la Commission Européenne : ………………………………… (précisez laquelle);
- Le ou les destinataires(s) adhérent aux principes du Safe Harbour;
- Le transfert de données a été autorisée par la CNIL et est encadré par les clauses contractuelles types établies par la Commission Européenne (préciser le numéro de la délibération autorisant le transfert);
- Le transfert de données a été autorisée par la CNIL et est encadré par des règles internes validées par la CNIL;
- La société bénéficie d'une des exceptions mentionnées à l'article 69 de la loi du 6 janvier 1978 modifiée en 2004 : ……………………………….. (préciser laquelle).

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée en 2004 relatives à l'informatique, aux fichiers et aux libertés, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service……………………………… *(citer le nom du service auprès duquel il est possible d'exercer son droit d'accès).*

Une difficulté ? Une hésitation ?

Pour plus d'informations, vous trouverez sur le site de la CNIL **www.cnil.fr**, rubrique « Déclarer » :

- un scénario en ligne d'aide à la déclaration
- tous renseignements utiles pour la désignation d'un CIL

Une permanence de renseignements juridiques par téléphone est assurée tous les jours de 10 heures à 12 heures et de 14 heures à 16 heures au **01 53 73 22 22**

Vous pouvez en outre adresser toute demande par télécopie au **01 53 73 22 00** (réponse sous 15 jours en moyenne)



www.cnil.fr

8, rue Vivienne - CS 30223
75083 Paris cedex 02
Tél. : 01 53 73 22 22
Fax : 01 53 73 22 00